Escorts Kubota Limited — Vulnerability Disclosure Policy

Policy owner: **Escorts Kubota Limited**

Contact: **psirt@escortskubota.com**

I. Overview

- The Escorts Kubota Limited Product Security Incident Response Team (hereinafter referred to as Escorts Kubota-PSIRT) is responsible for receiving, evaluating, and responding to vulnerability information related to products and services manufactured and provided by the company.

- This policy outlines our approach to handling reported vulnerability information, with the aim of enhancing the security of our products and providing users with appropriate risk mitigation measures.

- While we design our products with security in mind during development, this policy is intended to facilitate the acceptance of reports from users in the event that vulnerabilities are discovered.

- This policy may be revised without prior notice.

II. Scope

- This policy applies to Escorts Kubota Limited-branded agricultural Tractors, and their software, firmware, services, and supporting infrastructure (including Escorts Kubota Limited-managed servers and cloud services) from product release until the end of the manufacturer support period. It does not cover third-party products not under Escorts Kubota Limited control unless specified otherwise in vendor agreements/Contracts.

- The applicable period is from the product's release until the end of its support period (10 years).

- Vulnerabilities affecting official EKL diagnostic tools, update utilities, service applications, or software used for ECU programming are considered in scope.

- Below is the list of vulnerabilities which will be considered out of scope. When a reported issue could have a real, demonstrable impact on Escorts Kubota Limited systems or users, provide a concise proof-of-concept & we will reassess.

    - Exposed third-party client identifiers or secrets (e.g., SSO/OAuth IDs) without evidence they can be used to access Escorts Kubota Limited systems.
    - Clickjacking on pages that do not perform sensitive actions (no demonstrated impact).

- CSRF on unauthenticated, logout, or login endpoints where no privileged action is possible.
- Physical access alone does not automatically make a finding out of scope. Findings demonstrating unauthorized ECU access, diagnostic authorization bypass, firmware manipulation, CAN/J1939 abuse, security control bypass, or compromise of backend systems remain in scope.
- Reports identifying vulnerable components may undergo risk review at Escorts Kubota Limited's discretion. Vulnerable component identification alone does not guarantee acceptance or remediation.
- CSV/formula injection reports that do not include a reproducible exploit or tangible impact.
- SSL/TLS best-practice deviations (protocol/cipher recommendations) without an exploit demonstrating risk to Escorts Kubota Limited.
- Rate limiting or throttling concerns reported without a proof showing how they lead to account compromise, data exposure, or resource exhaustion.
- Content spoofing/text injection where the reporter cannot show control of rendered HTML/CSS or a realistic attack path.
- Social engineering alone is out of scope. However, security weaknesses facilitating malicious diagnostic package installation, unauthorized ECU programming, or dealership workflow compromise may be considered in scope.
- Session cookie reuse or open redirects that are only exploitable via phishing or other user deception.
- Open ports are out of scope unless they expose authentication weaknesses, sensitive services, configuration errors, or exploitable attack paths.
- Automated scanner output, CVE enumeration, fingerprinting results, or version-identification findings without manual validation and a working proof-of-concept.
- Physical penetration testing, DoS/DDoS testing, or any attack causing availability disruption.
- Presence or absence of the HTML autocomplete attribute on forms without demonstrated risk.
- Default, publicly documented, or manufacturer-provided credentials are out of scope unless they provide unauthorized access to systems or functions beyond their intended privileges.
- Independently operated dealer systems are generally out of scope unless they directly process EKL diagnostic services, software updates, ECU programming functions, or customer data managed on behalf of EKL.
- Purely mechanical, hydraulic, or other non-digital tractor subsystems. This exclusion does not apply where software, firmware, ECU logic, diagnostic commands, or network messages influence operation of the subsystem.
- Cache/CDN configuration issues attributable solely to third-party providers without demonstrable impact on Escorts Kubota Limited content or users.
- **Dangling IP Findings — Short Guidance**
  - Accepted (in-scope) dangling IP reports: considered only if the reporter provides clear, reproducible evidence of a security impact (for example, a practical subdomain takeover or the ability for an attacker to serve malicious content from the IP that affects Escorts Kubota Limited users or systems).

- Not accepted (out-of-scope): reports that merely show an IP was previously associated with Escorts Kubota Limited or is unassigned/unallocated, but do not demonstrate any exploitability, takeover, or traffic interception risk.

- **Minimum Reporting Requirements**
  - When submitting a report that could otherwise be borderline, include a concise proof-of-concept showing steps to reproduce, the real-world impact, affected product/component, and any supporting evidence (screenshots, request/response samples, or logs). Lack of a reproducible PoC is the most common reason for classification as out-of-scope.
  - If you believe a finding listed above has concrete impact on Escorts Kubota Limited, submit it with a short PoC and we will triage it promptly.

III. Reporting Vulnerability Information

- **Dedicated Contact Point for Vulnerability information reporting contact**
  - Please report any vulnerability information to Kubota-PSIRT using the following method: ・Vulnerability Submission Form

- **Acknowledgment and response**
  - As a rule, we will acknowledge receipt of reports as soon as possible.
  - Please note that if no contact information is provided in the customer information field, we will be unable to acknowledge receipt and share progress updates.
  - The company will not take legal action against reports made in good faith.
  - Additional information may be requested, if necessary.
  - The company does not operate a bug bounty program (reward system).

IV. Definition of Vulnerability

In this policy, a “vulnerability” refers to any issue that may adversely affect confidentiality, integrity, or availability due to program bugs, design flaws, or similar defects in our products (such as software, hardware, and firmware).

V. Information Required for Reporting

To facilitate smooth reporting, please provide the following information to the extent possible.

- Applicable product and version information (the product’s URL, lot number, etc.)
- Circumstances of vulnerability discovery (tools used, verification environment, etc.)
- Reproduction steps and PoC (Proof of Concept)
- Expected impact and threat scenarios
- Whether public disclosure is planned and the timing of such disclosure (e.g., conference presentation, blog post, etc.)

VI. Post-report Response Policy

- Escorts Kubota-PSIRT will review the reported details and collaborate with relevant departments to assess the impact and consider countermeasures.
- **Support type:** Update or replace ECU software.
- **Support method:** Distribute security patches via sales companies/dealers to implement ECU security measures.
- If the issue arises from a third-party component, we will coordinate with the relevant vendor and coordination organizations (e.g., CERT-In etc).
- Escorts Kubota Limited will provide status updates to the reporter at least every 30 days while remediation is in progress; more frequent updates may be provided where practical.
- The regular progress updates mentioned above will be communicated via email, telephone, or other appropriate means.

VII. Vulnerability Information Disclosure Policy

After completing the response, Escorts Kubota-PSIRT will disclose the following information on the company's official website.

- Applicable product and version
- Overview of the vulnerability (excluding technical details, such as exploit code and information that could lead to unauthorized use)
- Scope of impact and countermeasures as applicable.
- CVE number (if applicable).
- The CVE number will be obtained in coordination with (e.g., CERT-In etc) and communicated to the reporter.
- Credit will be given to the reporter, if requested. (anonymous reporting is also acceptable).

VIII. Legal Safe Harbor & Researcher Guidance

Escorts Kubota Limited will not pursue civil or criminal legal action against reporters acting in good faith and following the policy's terms. Good faith means: aiming to avoid privacy violations or data exfiltration of third-party personal data, not disrupting production services, and providing Escorts Kubota Limited reasonable time to assess and remediate before public disclosure. This safe harbor does not apply to activities that exceed the policy's permitted testing, deliberately harm persons or infrastructure, or involve clear unlawful conduct under applicable law.

IX. Use of Third Parties and Data Processors

Escorts Kubota Limited operates internal triage. If Escorts Kubota Limited engages third-party processors for security intake or vulnerability coordination, Escorts Kubota Limited

will use a Data Processing Agreement (DPA) and ensure GDPR-compliant safeguards for transfers of personal data from the EU to India, including appropriate transfer mechanisms (e.g., SCCs) where required.

X. Limitations and Disclaimers

This policy does not create contractual obligations or guarantees of timelines beyond Escorts Kubota Limited’s stated aims (for example, acknowledgment and update goals). Escorts Kubota Limited's obligations are limited to reasonable efforts to triage, investigate, and mitigate vulnerabilities. Nothing in this policy limits Escorts Kubota Limited’s legal rights under applicable Indian, EU, or other local laws. Where applicable EU CRA obligations require additional measures, Escorts Kubota Limited will follow the CRA for products sold in the EU market.